7.2 PASSWORDS AND SECURITY: DO HACKERS TEST ALL POSSIBILITIES?

Mark Zuckerberg, the founder and CEO of Meta Platforms (formerly Facebook, Inc.), is known to have kept “dadada” as his Twitter and Instagram passwords.Simple passwords of this type are a treat for hackers trying to gain access to an account. These passwords can be guessed in ashort amount of time by what is called a dictionary attack. In this case, an intruder tests common words and their combinationsuntil the correct password is found. What about more secure passwords? Is it possible to simply test all possibilities for a password and gain access to someone’s account? In this activity, we will estimate the time it would take to correctly guess a social media account password.

To start this activity, let’s assume that a social media platform requires your password meet the following requirements:

- Must have exactly 8 characters.
- Characters can be selected from any of the 26 letters of the alphabet, the numbers 0 through 9, and any of the characters #, $, %, or &.
- Repetitions are allowed.

1. Determine the number of distinct passwords that can be create using the rules described above. The number is very large, so you should use a calculator or computer for your computation.

Now, let’s assume that it takes 0.02 seconds to check a single possible password. Checking one password at a time is called a brute force attack.

2. How many seconds *could* it take to perform a brute force attack (if the hacker had to check every single password)?

3. How many seconds are there in a year?

4. How many years would it take to check every single possible password? Round your answer to the nearest whole year.

5. Let’s change the requirements of the password. Let’s say the first 4 characters must be letters, the next 3 characters must be digits, and the last character must be a special character from those listed above. How many distinct passwords can be created that meet these requirements?

6. How many years would it take to check every single possible password? Round your answer to the nearest whole year.

7. Let’s add another requirement. We still have to have the first 4 characters as letters, the next 3 as digits, and the last as a special character from those listed above, but now we cannot repeat characters. How many distinct passwords can be created that meet these requirements?

8. Are either of these new requirements more or less secure than the original conditions? Why do you think that?

9. What could a website do to make their password requirements more secure? Why would these requirements increase security?

10. Based on what you have found, do you believe hackers use the brute force attack method? Why or why not?